PCIG Consulting

Mobile and Remote Working Policy

Version: **1.0**
Date: **23 March 2020**

This template is for use by Practices to Comply with the GDPR requirement to have a policy regarding processing of patient data. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.

Change Control

Version	To	Change	Date
1			

Chapelgreen Practice

Mobile and Remote Working Policy

Document History

Document Reference:	
Document Purpose:	Mobile and Remote Working Policy
Date Approved:	
Version Number:	2.0
Status:	FINAL
Next Revision Due:	March 2021
Developed by:	Paul Couldrey – IG Consultant
Policy Sponsor:	Practice Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of Chapelgreen Practice or volunteering with the Practice.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2020

1.0 Introduction

1.1 This policy is intended to identify how Chapelgreen Practice will secure its data and its physical corporate assets when they are removed from Chapelgreen Practice premises for the purpose of staff working in remote locations, including working from home.

1.2 It will consider the physical security needed to protect valuable equipment and it will consider the electronic securities necessary to ensure that computers falling into wrong hands can't be used to access personal or other sensitive data.

1.3 It will also identify measures needing to be taken to ensure that data whether paper based or in electronic form is not able to be seen by unauthorised persons.

1.4 There maybe times such as the current pandemic situation for Co-Vid19 where practices will have to adopt a risk-based assessment on who can work from home, it is important to ensure patient services continue in the public interest. This and the safe of staff should be considered as highly as the protection of patient confidentiality.

2.0 Purpose

2.1 To ensure that Chapelgreen Practice and it staff comply with legislation and NHS standards in respect of information security and in particular the requirements of the NHS in respect of securing personal data and Chapelgreen Practice equipment which has to be transferred between sites or other organisations and which is to be used in locations other than in Chapelgreen Practice premises.

3.0 Statement of Intent

3.1 It is intended that Chapelgreen Practice complies with NHS and legal requirements for the securing of all information and physical assets whilst in transit and in use in locations outside THE PRACTICE's Premises. By doing so Chapelgreen Practice seeks to ensure the

- Confidentiality of personal information
- Integrity of information
- Availability of information

4.0 Scope and limitations

4.1 This policy covers all aspects of information being transferred or used outside THE PRACTICE, including but not limited to:

- Patient/client/service user information
- Personnel information
- PRACTICE information

4.2 This policy covers all aspects of using information, including (but not limited to):

- Paper based records
- Electronically held records on removable media or laptops which have been encrypted.

4.3 The policy applies to any person directly employed, contracted or volunteering to Chapelgreen Practice.

5.0 Objectives

- Ensure staff are aware of the need to determine the confidentiality and security of information in transit and that if moving and using information outside the Chapelgreen Practice environment, they ensure adequate security and working procedures are put in place, commensurate with the sensitivity of the information
- Ensure systems are in place to monitor all aspects of security and that these are reflected in the DS&P toolkit assessment
- Ensure training is in place to inform all staff of Information Security and to ensure they are aware of all their responsibilities with respect to the use of information and Chapelgreen Practice assets outside Chapelgreen Practice premises
- Ensure that no personal data in whatever form is lost as a result of using it outside of Chapelgreen Practice

5.1 The objectives of Chapelgreen Practice policy with regard to remote access by staff are:

- To provide secure and resilient remote access to THE PRACTICE's information systems
- To preserve the integrity, availability and confidentiality of THE PRACTICE's information and information systems
- To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security
- To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that Chapelgreen Practice is adequately protected under computer misuse legislation

5.2 The objectives of this policy with respect to mobile working are:

- To ensure all information, (but particularly personal confidential data) removed from THE PRACTICE's premises is kept secure
- To ensure all equipment removed from THE PRACTICE's premises is kept secure
- To protect individuals from risks associated with having information and equipment in their care when outside Chapelgreen Practice premises
- To identify basic rules for handling information and to provide guidance to managers as to how exceptions to those rules may be allowed

6.0 Duties

6.1 *Duties within THE PRACTICE*

6.1.1 The Caldicott Guardian is responsible for Information Security and the system of Internal Controls

6.1.2 The Caldicott Guardian will ensure that there are robust policies in place to ensure that patient information will remain confidential and be seen only by those

clinicians authorised to see that data. The Caldicott Guardian will ensure breaches of this policy with respect to patient information are investigated and will also ensure that Information Governance is duly regarded at Governing Body level when appropriate.

6.1.3 The GP identified as the Information Lead is the Senior Information Risk Officer (SIRO) who takes ownership of information risk and is a key factor in successfully raising the profile of information risk and in embedding information risk management into THE PRACTICE's culture.

6.1.4 Their responsibilities are: -

- To oversee the development of an Information Risk Policy, and a Strategy for the policy within the existing Information Governance Framework
- To take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control
- To review and agree action in respect of identified information risks.
- To ensure that THE PRACTICE's approach to information risk is effective in terms of resource, commitment and execution and that it is communicated to all staff
- To provide a focal point for the resolution and/or discussion of information risk issues

6.1.5 Chapelgreen Practice Manager will, through the Data Security and Protections Toolkit, ensure that Chapelgreen Practice has robust policies, procedures, strategies, training and awareness programmes and monitoring schedules in place to ensure the confidentiality, integrity and availability of data and ensure that Chapelgreen Practice complies with relevant current legislation.

6.2 Responsibilities of other staff

6.2.1 **All Staff** will ensure that they have read this policy and have undertaken the relevant mandatory training in the subject of Information Governance

6.2.2 In addition all staff will abide by the policies and the procedures, regarding information, which have been ratified by Chapelgreen Practice as well as all legislation and law.

7.0 Definitions

IAA	Information Asset Administrator
IAO	Information Asset Owner
Mobile Working	Mobile working refers to the moving around of information on a laptop/other portable media and/or hard copy because this is necessary in order to carry out one's function effectively and efficiently
PCD	Personal Confidential Data
Remote Access	This refers to any technology that enables users to connect securely in geographically dispersed locations and supports mobile working e.g. normal place of work and including working from home. This access is typically over some kind of dial-up connection, broadband or 3G link through a terminal server. This gives the effect of working directly onto the network in the workplace and depending upon what access rights are given, access to emails, files and the intranet can be made. For email the possibility of using web mail is available.
Remote working	Accessing THE PRACTICE's information systems from other than one's normal place of work, including home, possibly taking hard copy material outside of THE PRACTICE's premises in order to do so - because this is necessary in order to carry out one's function effectively and efficiently
SIRO	Senior Information Risk Officer

8.0 Remote Access and Mobile Working

8.1 The following information is applicable to all staff who use mobile computing devices such as Laptops, Memory Sticks, Tablet PC's, PDA's cameras, mobile phones, satellite navigation systems and any other piece of electronic equipment capable of holding names, addresses or other details.

8.2 This policy covers all types of remote access, whether fixed or 'roving' including:

- Travelling users (e.g. Staff working across sites or temporarily based at other locations)
- Home workers (e.g. Clinicians)
- Non NHS staff (e.g. Social Services, contractors and other 3rd party organisations)

8.3 In addition it is recognised that not all information used away from THE PRACTICE's premises is accessible through computer or electronic means. Some of that information can be paper based, e.g. health records for seeing patients at other locations or in the patient's own home, or staff files being used by staff whilst working at home.

9.0 Security of Corporate Information

9.1 In order to ensure adherence to the General Data Protection Regulation (GDPR) the following guidelines must be followed:

- As a general principle of good practice, patient or staff identifiable information should not be stored on a mobile computer and certainly must not be stored on one unless it is encrypted to the standards required in the Encryption Policy
- **Under no circumstances should any patient based personal information be stored on any device other than equipment provided by THE PRACTICE e.g. laptop or digital camera. Mobile phones containing cameras, personal or work provided will not be used to take or store patient images or to transmit such images. Similarly no patient information will be stored on personally owned equipment such as iPods, PDA, Satellite Navigation Devices etc**
- If PCD must be stored on a mobile computer, then the general principles about sensitive information given above must be followed
- PCD obtained through work must only be stored on computers, electronic equipment or electronic media that are the property of Chapelgreen Practice and therefore are subject to the policies and procedures of THE PRACTICE
- Loss of a mobile computer holding confidential information must be reported through the Incident Reporting mechanism as soon as possible. Chapelgreen Practice has responsibility for informing staff or patients if their personal information has been disclosed unlawfully
- Devices holding sensitive information must be encrypted in order to safeguard the information against unauthorised access. Encryption must be done to the standards currently required by THE PRACTICE
- Sensitive information should be removed from the device as soon as practically possible
- Patient identifiable information on mobile devices should be kept to a minimum i.e. use a hospital/NHS number instead of a name wherever possible, this is to reduce the risk of breach of confidentiality if the device is lost or stolen.
- Information stored on laptops should be regularly backed up and the backups held within a secure location. Normally data should be backed up regularly to a secure location on THE PRACTICE's network. **This would involve regular synchronisation of the computer when connected to the network**
- All mobile devices must be authorised for use by IT Service Provider before connection to either a PC or the network is allowed
- Mobile devices should be password protected to ensure that unauthorised use cannot occur. Passwords should not be shared. If your password is compromised please report immediately to IT Services
- Virus protection software must be installed, active and up to date

10.0 Manually Held Records

10.1 As part of remote or mobile working, it is often necessary that paper based records are available. This would be the case for treating patients in their own home, in the case of clinical records, or when attending tribunals, in the case of staff records.

10.2 It is necessary that these records are handled with due care and responsibility and the following points may assist in this:

- Use a case or sealed envelope or wallet to ensure the papers are kept together and nothing can blow away
- Don't leave files in an unattended car, even when they are locked in the boot and out of sight
- Transport documents directly to and from the place of work to the client's address. Don't make stops, for example at the local supermarket
- Return files to the work location at the end of the day, if possible.

  Don't take them home. However, locally this may need to be carefully considered if it would cut down the number of visits someone can make because of extra travelling to collect the documents at the start of the day. Local procedures will identify those occasions on which the department management will allow such exceptions to the basic rule of not taking PCD home. These procedures should be authorised at **partner level**.

Appendix 1 provides pro-forma to authorise removal of personal data

- If documents are taken home at the end of the day, they must not remain in the car, even if it is locked in the garage. Bring the documents into the house and store them in what you consider to be a safe location. This should be somewhere where other occupants of the house will not casually look through them. A possible location would be where you keep your purse or wallet whilst in the house. They should not be left adjacent to doors or windows
- If visiting a number of clients in the course of the day, consider taking all files with you to each visit, rather than leaving in car
- Travel with car doors locked. A boot could easily be opened by someone at a set of traffic lights, as could a passenger door
- All losses of personal data recently have occurred as a result of people not following policies and procedures

11.0 General principles of removing manual records and equipment for remote access

11.1 As a general principle, PCD or sensitive information should not be taken off site and used remotely. This includes manual records and equipment needed to access such electronically held records. However, if this is deemed necessary due to emergency requirement -data should be stored securely at the home – and used for work purposes only and SHOULD NOT be available to other members of the household.

11.2 However there are going to be exceptions to this where it is necessary for the purposes of enabling relevant work to be undertaken e.g. home visits and working on HR issues on other sites. For these papers or the computers necessary to access such information will have to be carried around. During pandemic situations.

11.3 Under those circumstances a member of staff must not make an arbitrary decision to remove those documents, but for regular occasions local policies and procedures must be developed for the handling of the notes and information.

11.4 There will be occasions when it is necessary for staff to take notes or sensitive information home, in order to make an early morning appointment at patient's homes, or in the evening when late appointments prevent documents being safely returned to their normal library location. Again, if locally allowed, the local procedures must document what is permitted. However, it is re-iterated that as a default this is not an acceptable practice.

11.5 On an occasion which constitutes an unusual event e.g. when a member of staff is required to undertake work on a one off basis outside of THE PRACTICE, and which necessitates the use of sensitive or personal data, the authority to take the information or the equipment necessary to access that information must be documented. This authority will be granted by their line manager and will include the date and time during which that information is removed from site, the nature of the information to be removed and the reasons why it is being allowed to be removed Similar information will also be recorded for the removal of equipment necessary to access such information from a remote location.

11.6 In all instances where sensitive information has to be taken, or accessed off site, the user must have completed the mandatory information governance training and shown an understanding of the security issues at stake.

11.7 Any local policy approving the use or removing of sensitive information from the THE PRACTICE's premises must be approved by the Caldicott Guardian.

12.0 Personal Health & Safety Applicable to Mobile Working Environments

12.1 The following legislation is applicable to working in remote locations as well as for working in a regular work situation:

- The Management of Health & Safety at Work Regulations 1999: requires employers/employees to assess risks to their health and safety by ensuring that all reasonable controls are put in place to enable safe working
- The Display Screen Equipment Regulations 1992: do not advocate the use of mobile equipment due to the inability to achieve an ergonomic layout; therefore the use of laptops/PDA should be minimised to short and infrequent spells throughout the working day
- The Manual Handling Operations Regulations 1992: should be borne in mind whilst carrying/moving/using the equipment so as to ensure sensible posture is maintained rather than repetitive awkward postures that may culminate in pain/discomfort. To achieve compliance the following actions can be undertaken when moving equipment:
- Use a carrying aid e.g. use the laptop case that has been specifically designed to distribute the weight of the laptop to reduce strain on the body
- Only carry essential items
- Reduce the distance that items have to be carried e.g. by parking as close as possible to the given location.

- All lifting and handling will be done in compliance with the Moving and Handling Policy.
- Manual records should be locked away when not in use.

12.2 A laptop computers is a prime target for theft because it is a valuable item that can be easily snatched. In addition, any documentation needs to be protected against theft or loss. The following actions although not exhaustive should be considered:

- Where possible, the location should be well lit and adequate parking arrangements made wherever possible
- Valuable equipment should be disguised or hidden from view. This prevents advertising valuable equipment to thieves
- Staff should report suspicious activity and notify incidents so that other staff are aware
- Staff should read and comply with the Lone Working Policy
- It may be useful for staff to carry mobile phones and personal attack alarms in case of emergency
- Computers and documentation containing personal or sensitive information should be carried in the locked boot of a car not on the seat of the car from where it can be snatched
- Journeys should be direct from the work location to the place of remote working. Stops should not be made at supermarkets etc whilst carrying such assets or documentation
- Lock the car doors to increase security when stopping temporarily at traffic lights
- Do not leave computers, removable media or sensitive documentation in the car overnight, even if it is garaged
- Avoid heavy jolts during transit which may render the system inoperative
- When the system is in operation, display a NHS sticker, to ensure NHS material will be recovered from your vehicle following an accident. Mobile devices must be clearly labelled with a return address. Ultraviolet marking of equipment would also be considered good practice
- Only retrieve, use or carry as much data as you need. The more files or records (electronic or manual) the greater the risk of something falling into the wrong hands

13.0 Securing the Data and Computers in the Home

13.1 Having ensured that the data and mobile media or laptops have arrived in the location in which they are going to be used, there is now a need to ensure the sensitive data remains secure and not seen by others who may live in the house. This must be done in accordance with the Flexible Working Policy and THE PRACTICE's requirements for home working.

13.2 All health and safety aspects of the working environment must also be complied with.

13.3 In addition the use of sensitive or personally identifiable data must be controlled in such a way that approval must be given for its "offsite" use. A casual approach to its removal is no longer acceptable, even when it is encrypted.

13.4 The following guidelines identify what is, and what isn't acceptable in respect of using data in a home or remote environment:

- A basic principle across Chapelgreen Practice is that no PCD will be taken off site for any other purpose than the treatment of patients or because meetings requiring access to specific personal data are taking place
- As a further principle, any PCD taken off site for specific purposes identified above will be returned the same day to the secure work location, where it will be locked away
- It is recognised that for Chapelgreen Practice and many of its staff to operate efficiently, it is necessary for PCD to be taken home so that meetings external to Chapelgreen Practice can be attended in the early morning or in the late afternoon, when it would be very inconvenient to return to the work environment. Under these circumstances, the person taking the PCD off site should notify their manager as to what is being removed, for how long and for what reason
- People also have a need to work from home and need to have access to documentation containing PCD in order to undertake that work. In line with the Flexible Working Policy, it is necessary that the package of work is agreed with the manager and at the same time agreement for the removal of the required PCD can be made
- Users of PCD should have available an email from their manager agreeing to the use of that PCD in a remote or home location
- Accessing of PCD through the use of a computer linked to the network is as easy as accessing the information in a work environment, but again the user must have emailed agreement for the use of that information. Logs of user's time on the network will identify potential problem areas if data is lost

13.5 There are some basic principles which apply to working in a remote or home location whether the information being used is sensitive or not:

- Do not allow any other person to use or play with the computer regardless of whether it is logged in or not
- Ensure others do not read the content of the screen
- Do not allow others to read through any documentation which you may be using
- Log off the computer when not using it or at least lock it using the Ctrl+Alt+Del keys
- Do not leave papers lying around. Tidy them away (and store somewhere safely if overnight).

- Do not share passwords with anyone else
- Dispose of information safely when working remotely making sure that confidentiality is maintained. If possible, shred any sensitive papers when no longer required or return them to be disposed of in line with Chapelgreen Practice policy.
- Be careful when having telephone conversations with colleagues about work whilst in a remote location, that the conversation cannot be overheard

14.0 Reporting Security Incidents & Weaknesses

14.1 Reporting of any losses, theft or damage to documentation or computer assets will be through Chapelgreen Practice Manager at the first possible opportunity, and with a degree of urgency. This should then be reported to Chapelgreen Practice Data Protection Officer (DPO)

14.2 Information provided will include details of the losses or incidents and a detailed description of the data lost. Any PCD lost will need to be reported to the DS&P as a Breach and individual subjects will need to be notified of the losses. Please refer to the Breach Reporting Policy.

14.3 Near misses and possible weaknesses will also be reported through this method.

15.0 Disciplinary Issues

15.1 The loss of personal information within the NHS is treated very seriously; reports having to be made to the CCG, and Chapelgreen Practice have to make declarations within their annual report to the DS&P toolkit of any breaches of information security.

15.2 It is therefore reasonable that disciplinary action should be taken against anyone found to have wilfully or neglectfully put sensitive data or equipment capable of accessing sensitive data at risk.

15.3 In the context of this policy there are two forms to the misdemeanours that can occur:

1. People who are not approved to take equipment or papers off site but who do so and thus break the rules laid down in this policy

2. People who are approved to take papers or remote access equipment off site but who then fail to observe the rule in this policy aimed at protecting the data and equipment

15.3.1 In either case, sensitive information can be put at risk and in line with THE PRACTICE's policies, disciplinary action will be taken, and charges of gross misconduct brought.

15.4 In addition any breach of security which may occur in respect of PCD will if they meet the requirements be reported to the Office of the Information Commissioner under the specifications of the GDPR -advice should be sought from Chapelgreen Practice DPO.

15.5 All staff are subject to the terms of this policy.

16.0 Dissemination, Implementation and Access

16.1 Dissemination of this policy will be undertaken by publishing on the Intranet.

17.0 Monitoring Compliance

17.1 Staff are expected to comply with the requirements set out within the Mobile and Remote Working Policy and related policies. Compliance will be monitored by Chapelgreen Practice Manager with reports of spot checks, completion of staff questionnaires, incidents reported, electronic audit trails and submission of the DS&P Toolkit.

17.2 Non-adherence to the Mobile and Remote Working Policy and related policies will result in disciplinary action being taken.

18.0 References

- Access to Health Records Act 1990
- General Data Protection Regulation 2016
- Data Protection Act 2018
- Crime and Disorder Act 1998
- Human Rights Act 1998
- Common law duty of Confidentiality
- Freedom of Information Act 2000
- Criminal Procedures and Investigations Act 1996
- Regulation of Investigatory Powers Act 2000
- Health and Social Care Act 2001 (Section 60)
- NHS (Venereal Disease) Regulations 1974
- Human Fertilisation and Embryology Act 1990
- Abortion Regulations 1991
- Data Protection Act Policy and Procedures
- NHS Code of Practice: - Confidentiality (Inc Caldicott)
- Children's' Act 2004
- Mental Health Act 2007
- Management of Health and Safety at Work Regulation 1992
- Health and safety (Display Screen Equipment) Regulation 1992
- Manual Handling Operations Regulation 1992

19.0 Appendix 1

Authority to Take Personally Identifiable Data Off-Site

This document provides the authority for the named member of staff to remove Personally Confidential Data (such as patient data) and not to return it to the work place at the end of the working day. This is an exceptional instance intended to facilitate particular circumstances which prevent the named person from either returning to the work place at the end of the day or to facilitate early morning visits or meetings when it is not possible for the named member of staff to attend the work place in the morning.

This document does not absolve the member of staff from taking good care of the documentation and abiding by all other aspects of the Mobile and Remote Working Policy.

Name of Staff Member authorised to remove data.
Details of Information to be removed.
Reason for removing Information
Name of member of Staff authorising removal
Date of return of Information
Signature and Date of authorised member of staff Date
Signature of authorising member of staff Date